Department of Homeland Security IAIP Directorate Daily Open Source Infrastructure Report for 14 June 2005

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
http://www.dhs.gov/

Daily Highlights

- Reuters reports two computers containing personal information on Motorola employees were stolen from the mobile phone maker's human resources services provider, the latest in a series of incidents of companies losing control of employee data. (See item 4)

- The Charleston Daily Mail reports the West Virginia Department of Agriculture wants cattle across the state fitted with radio identification ear tags in an effort to monitor their locations should there be an outbreak of mad cow or other disease. (See item 10)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *June 13, Associated Press* — **OPEC may increase production ceiling.** The Organization of Petroleum Exporting Countries (OPEC) is expected to raise its daily output quota by half a million barrels when it meets Wednesday, June 15, though analysts said the move would have little impact on oil prices, which are now about $55 a barrel. The anticipated increase would bring the official quota to 28 million barrels per day −− a symbolic gesture, analysts said, since the cartel is already pumping that much. Analysts say the underlying reason for today's high prices is not a shortage of oil, but rather the petroleum industry's limited excess production capacity, which leaves only a limited supply cushion in the event of an unexpected disruption. The war in Iraq, labor unrest in Nigeria and political uncertainty in Russia and Venezuela have

made oil traders uneasy for about two years. Rising demand, particularly in China and the United States, have also contributed to the market's nervousness. Saudi Arabia is the only known country in the group with the ability to add barrels to daily production. But the kingdom's oil minister, Ali Naimi, says that even if the Organization of Petroleum Exporting Countries raises its production ceiling, it may not make sense to add actual oil to the market. He attributes the high prices to bottlenecks in the worldwide refining system.
Source: http://www.signonsandiego.com/news/business/20050613−1056−op ecmeeting.html

2. *June 13, Government Technology* — **Tennessee state parks harness the Internet for energy management.** The managers at Fall Creek Falls State Park know exactly how much electricity was used at the park yesterday, and they didn't have to leave their offices to read a meter. The managers at Fall Creek Falls State Park know exactly how much electricity was used at the park yesterday, and they didn't have to leave their offices to read a meter. All they did was turn on their computer and log into a Website provided by the local electric utility, Sequachee Valley Electric. The monitoring system will allow Fall Creek Falls managers to track their energy consumption to ensure efficiency. And with recent lighting and cooling improvements as well as the purchase of green power, energy efficiency at the park is getting even better. The solution is a Web−based energy information service provided by Automated Energy. Information goes directly from the meter to the Internet by phone line. Sequachee Valley Electric is one of the first electric utilities in Tennessee to bring Web−based information services to its customers, following the lead of Nashville Electric Service, which started its PowerTracker program a few years ago.
Source: http://www.govtech.net/news/news.php?id=94266

[Return to top]

Chemical Industry and Hazardous Materials Sector

3. *June 12, Associated Press* — **Nerve agent spills at Indiana facility.** About 30 gallons of a liquid containing a deadly Cold War−era nerve agent spilled at an Indiana chemical weapons depot, but it was safely contained in a sealed area and no one was injured, the Army said Saturday, June 11. The spill occurred Friday night at the Newport Chemical Agent Destruction Facility, where more than 250,000 gallons of the agent VX are stored. VX is a liquid with the consistency of mineral oil that can kill a healthy adult with a single pinpoint droplet. The spill happened during a process to destroy the nerve agent by converting it into a caustic chemical called hydrolysate. The facility has destroyed nearly 2,900 gallons of VX since the process started a month ago, the Army said. The neutralization process is expected to take more than two years. Workers would try to determine what caused the valve to leak Friday night and how to fix it, said Army spokesperson Terry Arthur. "No agent was released outside the containment area and there was no danger to workers or to the community," the Army said.
Source: http://abcnews.go.com/US/wireStory?id=841679

[Return to top]

Defense Industrial Base Sector

Nothing to report.

[Return to top]

Banking and Finance Sector

4. *June 13, Reuters* — **Two computers stolen with Motorola staff data.** Two computers containing personal information on Motorola Inc. employees were stolen from the mobile phone maker's human resources services provider, Affiliated Computer Services, the latest in a series of incidents of companies losing control of employee data. The data on the stolen computers included names and Social Security numbers but no financial information, according to Motorola. The number of employees affected was not disclosed. "All employees were notified, but to this date there is no indication that any personal information has been compromised," said ACS' chief marketing officer, Lesley Pool. ACS said thieves broke into its office in the Chicago area over the May 38−30 Memorial Day weekend and stole the computers. Police are investigating, it said. Motorola said it had e−mailed all of its U.S. employees alerting them to the incident. According to Motorola, the computers had strong security safeguards that made it difficult to access the information. Employees affected by the theft are mostly in the United States, home to about half of Motorola's global work force of some 68,000.
   Source: http://www.eweek.com/article2/0,1759,1827276,00.asp

5. *June 13, News−Gazette (IL)* — **Counterfeit money showing up in East Central Illinois.** Counterfeit bills −− mostly $100s and $20s −− have been appearing frequently in East Central Illinois. Eric Pingolt, resident agent−in−charge for the U.S. Secret Service in Springfield, IL, said citizens and merchants need to pay attention to the currency they receive. "If an individual receives a bill that they suspect may be counterfeit, they should notify their local law enforcement immediately," Pingolt said. Pingolt said there have been quite a few phony bills recovered in recent months, with counterfeit $20s being the most common. Secret Service agents are working with police in Champaign, Urbana and elsewhere in East Central Illinois and have some leads they are pursuing.
   Source: http://www.news−gazette.com/localnews/story.cfm?Number=18407

[Return to top]

Transportation and Border Security Sector

6. *June 13, Associated Press* — **American Airlines protects pensions.** When American Airlines teetered on the brink of bankruptcy in 2003, employees agreed to $1.8 billion worth of concessions, with one comforting condition: their pensions would be protected. That deal, which saved the nation's largest carrier from a Chapter 11 filing, is a key factor that distinguishes American from its rivals at a time when the retirement benefits of workers throughout the industry are increasingly at risk. UAL's United Airlines and US Airways Group have dumped their pension plans through bankruptcy restructuring, and other carriers are threatening to do the same. The chief executives of Northwest Airlines and Delta Air Lines on Tuesday, June 7, told senators that their companies may have to seek bankruptcy court protection unless Congress gives them a 25−year extension to meet multibillion−dollar funding

gaps in the pension benefits promised to workers. Delta tops the list of U.S. airlines with under funded pensions, with a deficit of $5.3 billion, according to Standard & Poor's. Northwest is next in line with a funding deficit of $3.8 billion, while American has a shortfall of $2.7 billion.
Source: http://www.usatoday.com/travel/news/2005−06−13−aa−pensions_x .htm

7. *June 13, Reuters* — **United's cost cuts may tempt rivals to try Chapter 11.** After 2 1/2 years in bankruptcy, United Airlines is poised to emerge in the fall with an enviable cost structure that could tempt rival carriers to strive for similar cost cuts through court protection. United, a unit of UAL, has made the most of Chapter 11, reducing yearly costs by $7 billion. US Airways Group, also bankrupt, has won more than $1 billion in annual labor savings this year, an amount that might have been impossible outside of bankruptcy. The savings of those two carriers has put increased pressure on non−bankrupt rivals, battered by soaring fuel prices and low−fare competition, to slash costs as well. Delta Air Lines, at risk of a bankruptcy filing, is seeking $5 billion in annual savings. Continental Airlines hopes to cut labor costs by $500 million a year. Northwest Airlines hopes to wring $1.1 billion from its labor force as it restructures, but has run into strong resistance from labor unions. Experts said that if airlines are unable to match UAL's cost cuts outside of Chapter 11, then they may well take the bankruptcy route themselves. But experts warned that bankruptcy is not a guaranteed remedy for what's ailing airlines. With a relatively low rate of successful restructuring, some industry leaders consider it strictly a last resort.
Source: http://www.usatoday.com/travel/news/2005−06−13−united−bankru ptcy_x.htm

8. *June 13, USA TODAY* — **Fliers fill seats despite higher fares.** The struggling "Big Six" U.S. air carriers last month managed to pack planes to a record level again despite modest fare increases. The traditional airlines −− American, United, Delta, Northwest, Continental and US Airways −− filled 79.2% of their seats, according to an analysis by Back Aviation Solutions for USA TODAY. That tops the previous May record of 76.3% last year. The new number extends a period of more than a year in which airliners have been flying fuller than normal. It also means May was among the fullest months ever for the Big Six. The fullest: July 2004, when the big airlines jammed their planes 84% full. On the cusp of summer vacation season, ticket sales remain strong, and travelers' chances of being next to an empty seat are dim. "We're going to have a very busy summer," says Michael Allen of Back. Passengers, meanwhile, have been largely undeterred by a series of recent small fare increases, says Terry Trippler, an airline expert at CheapSeats.com. Airlines have raised fares seven times since February. "There are many leisure fares in many markets that are $40 to $50 higher (round trip) than they were in February," Trippler says.
Source: http://www.usatoday.com/travel/news/2005−06−12−fliers−fares_ x.htm

9. *June 10, Department of Transportation* — **Money for Beartooth Highway repairs.** Department of Transportation Secretary Norman Y. Mineta approved an initial $2 million in emergency relief funds to jump−start repairs to Beartooth Highway in the aftermath of mudslides that closed this gateway to Yellowstone National Park, it was announced on Friday, June 10. The $2 million is available immediately for the Montana Department of Transportation to clear debris, shore up embankments and install rock fall prevention measures on parts of the highway. The full cost of the highway's repair, estimated at approximately $20 million, will be eligible for federal reimbursement. The emergency relief program provides funding for the repair or reconstruction of federal−aid highways and roads on federal lands that have suffered

serious damage as a result of natural disasters or catastrophic events. Mineta said that he has proposed raising the emergency relief funding level from $100 million to $250 million per year as part of the six−year, surface transportation reauthorization bill now before Congress to further assist states facing emergencies such as this.
Source: http://www.dot.gov/affairs/dot8605.htm

[Return to top]

Postal and Shipping Sector

Nothing to report.

[Return to top]

Agriculture Sector

10. *June 13, Charleston Daily Mail (WV)* — **Agriculture department seeks to tag all West Virginia cattle.** The West Virginia Department of Agriculture wants cattle across the state fitted with radio identification ear tags in an effort to monitor their whereabouts. "We're mainly preparing ourselves for an outbreak of mad cow disease," said Buddy Davidson, the agency's communications officer. Davidson said the advantage of ear tags is that they enable animals to be traced more rapidly. Mad cow is a fatal degenerative disease that affects the central nervous system of adult cattle. The U.S. Department of Agriculture has diagnosed only one case of the disease in the United States, in a dairy cow in Washington state in December 2003. In the event of an outbreak, an infected herd could be found in 48 hours with ear tags. This would be a considerable improvement over the two weeks it took to locate an infected dairy cow in the state of Washington. Davidson said every farm and slaughterhouse in West Virginia will have an ID number. Wherever the cattle go, they'll be scanned and that number will be recorded electronically, Davidson added. The numbers will be part of a state database that eventually will be part of a national database. Participation by farmers is voluntary.
Source: http://www.dailymail.com/news/News/2005061312/

[Return to top]

Food Sector

11. *June 10, just−food.com* — **Japan's Nippon Flour Mills buys U.S. pasta company.** Nippon Flour Mills of Japan has bought California pasta maker Costa Macaroni Mfg Co for $3.1m, according to the Nihon Keizai Shimbun newspaper. Nippon Flour Mills will use Costa's to broaden its sales territory in the U.S., the paper said. Nippon Flour Mills acquired the company through its U.S. subsidiary Pasta Montana. With the purchase, Pasta Montana will have access to about 200 firms that are client companies of Costa. To date, Pasta Montana has sold its products chiefly in the northern region of the U.S. West Coast, including Seattle. It hopes to broaden its reach in California with the purchase.
Source: http://www.just−food.com/news_detail.asp?art=60978

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

12. *June 13, Herald Sun (Austrailia)* — **Bird flu test provides quicker results.** Australian scientists have developed the fastest way to identify the potentially deadly bird flu. Researchers have cut the time taken to confirm avian influenza from three weeks to just one day. The breakthrough will allow authorities to act swiftly to control an outbreak if it hits Australia. The test, developed by Department of Primary Industries experts, is capable of detecting 15 sub−types of avian influenza, including several strains lethal to humans. Australian Agriculture Minister Bob Cameron said Monday, June 13, the breakthrough means enormous health and financial benefits. Any outbreak could threaten Australia's $430 million poultry industry, potentially affecting 3000 jobs, he said. While there have been no cases of bird flu in Australia in five years, more than 50 victims have been reported in South−East Asia. Cameron said the new tests would be of greatest benefit to countries on the fringes of Asia.
Source: http://www.heraldsun.news.com.au/common/story_page/0,5478,15 605193%255E2862,00.html

13. *June 13, Sacramento Bee (CA)* — **Authorities confirm no specific terrorist threat to California hospitals.** The California Department of Health Services reassured hospitals that they were not a potential target of a possible terror attack on Thursday, June 9, but the department also encouraged heightened security. In letters faxed overnight Wednesday to 440 hospitals statewide, the Department of Homeland Security (DHS) said: "We have confirmed that there is no information regarding any specific or defined threat against hospitals." State health officials said they faxed the letters to counter some media reports of an affidavit in the Lodi, CA, terror probe that named hospitals as "potential targets for attack." The DHS letters also list "suggested protective measures" to tighten security. Many of the precautions −− identification badges for visitors, inspecting packages, and restricting access to lab supplies and radiological material −− became standard procedure after the attacks of September 11, 2001. This spring, hospitals stepped up security after the DHS warned that individuals posing as health inspectors had entered hospitals in Boston, Los Angeles and Detroit and tried to collect confidential records. On Thursday, California hospitals received a homeland security bulletin reminding them of the fake inspectors and advising them to take precautions identical to those faxed out by California health officials.
Source: http://www.securityinfowatch.com/article/article.jsp?siteSec tion=306&id=4445

14. *June 09, Albuquerque Tribune (NM)* — **Study's authors to focus on airborne bacteria.** Scientists and doctors have little experience or information to guide them in protecting people from bioweapons, even those made from relatively common bacteria. But a new, $15 million, five−year grant from the Department of Health and Human Services to the University of New Mexico (UNM) and Lovelace Respiratory Research Institute could change that, said Rick Lyons, a UNM Health Sciences Center professor. The grant will let the two organizations study

how agents like anthrax, plague and smallpox affect the lungs, Lyons said. The organizations will use lung cell culture and rodent studies to see how airborne bacteria affect the body. The work will be done in UNM's Bio−Safety Level 3 lab, which the university has operated for the past 12 years, and similar facilities at Lovelace, Lyons said. "We've actually been working with these bacteria as a health problem and things like hantavirus for several years," Lyons said. "Things like anthrax normally infect the skin, which isn't such a big deal. But by understanding what they do to the lungs and knowing how the lungs work to defend themselves, we should be able to find better ways to fight enhanced forms of these bacteria."
Source: http://www.abqtrib.com/albq/nw_local/article/0,2564,ALBQ_198 58_3842657,00.html

[Return to top]

Government Sector

Nothing to report.

[Return to top]

Emergency Services Sector

15. *June 13, WAVE3 (KY)* — **Companies in Kentucky stage terrorism drill.** Companies in Louisville, Kentucky's, Rubbertown neighborhood staged a terrorism drill Monday, June 13. Local firefighters, emergency responders and law enforcement officials joined Dupont employees for the series of exercises, which were staged at the DuPont chemical plant. During one drill, intruders had broken into the plant, and firefighters had to deal with a flaming pit filled with diesel fuel. A second drill involved containing a leak from two tank cars containing toxic chemicals. The Rubbertown Mutual Aid Association has been staging the drill every three years, but it took on added urgency after the terror attacks of 9−11. The drills will continue through Wednesday as part of a nationwide terrorist preparedness effort organized by the FBI, Department of Defense and Department of Homeland Security.
Source: http://www.wave3.com/Global/story.asp?S=3467114&nav=0RZFayCw

16. *June 12, The Journal News* — **New York county puts new drill to the test.** Police in Westchester County, NY, on Saturday, June 11, held the first countywide mutual aid drill since the testing system was revised nearly a year ago. In the surprise morning drill, county police put out a mock alert about a plane crash at Westchester County Airport in Harrison, requesting aid from police departments in the county. A year ago, the Westchester Police Chiefs Association revised the mutual−aid plan with an eye toward responding to terrorist attacks and other major emergencies. The more recent plan accounts for extra police sources and deployment changes that have occurred over the years. The drill was designed to measure the resources available to the county, response times and the effectiveness of the levels of command. Altogether, 110 officers from 50 departments responded to the scene from as far as Mount Vernon. They included police from the Metropolitan Transportation Authority and the Department of Environmental Protection.
Source: http://www.thejournalnews.com/apps/pbcs.dll/article?AID=/200 50612/NEWS02/506120345/1018

17. *June 11, WISTV (SC)* — **Civil Air Patrol prepares for active South Carolina hurricane season.** The Civil Air Patrol in South Carolina is bracing for "Hurricane Steve." But Hurricane Steve is a part of the Patrol's disaster response drill. As part of the drill, 13 small planes are sent out through the state, each one with a mission to provide aid on the ground and the air. Major Owen Barker explains it's a unique group, "One of the things that are so nice about the Civil Air Patrol, all individuals are strictly volunteers. They give of their time and their resources that really help the state all the citizens of the state." As one way of preparing, visual images were taken of the Midlands from the Civil Patrol Aircraft. Pilot Barker says the pictures would be essential in the event of real hurricane, "It would be important for the people at the Emergency Management Division to have real photos of the damage that has been done as hurricane passed through an area."
Civil Air Patrol Website: http://www.cap.gov/
Source: http://www.wistv.com/Global/story.asp?S=3462643&nav=0RaPavvK

[Return to top]

Information Technology and Telecommunications Sector

18. *June 10, internetnews* — **Hackers deface Korean Mozilla Website.** The Korean language Mozilla Website was hacked and defaced last week, prompting calls from some corners of the open source community to gain control of the independent site. The job was likely the work of the notorious Simiens Crew, a Brazil−based outfit, and while the main page was not affected, other pages were replaced by the message "Simiens Crew ownz u viva os macacos." The phrase "os macacos" means "the monkeys" in Portuguese. It could be that the hackers simply have misspelled their own name, according to MozillaZine, a Web−based forum for the browser's enthusiast. The proper spelling is "Simians" and means apes. The crew has attacked several high−profile sites, often exploiting a vulnerability in the AWStats log file analyzer, according to MozillaZine. While Mozilla Europe, Mozilla Japan and Mozilla China have an official affiliation with the foundation, the Korean language Website has no official connection. Channy Yun, leader of Mozilla Korean Community, said the hack happened because there was not a patch for a PHP vulnerability for the company hosting mozilla.or.kr. He assured users he would backup and fix the problem with the ISP.
Source: http://www.internetnews.com/security/article.php/3512081

19. *May 13, Government Accountability Office* — **GAO−05−231: Information Security: Emerging Cybersecurity Issues Threaten Federal Information Systems (Report).** Spam, phishing, and spyware pose security risks to federal information systems. The blending of these threats creates additional risks that cannot be easily mitigated with currently available tools. Most agencies were not applying the information security program requirements of the Federal Information Security Management Act of 2002 (FISMA) to these emerging threats. Pursuant to FISMA, the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS) share responsibility for the federal government's capability to detect, analyze, and respond to cybersecurity incidents. However, governmentwide guidance has not been issued to clarify to agencies which incidents they should be reporting, as well as how and to whom they should report. The Government Accountability Office (GAO) recommends that the director, OMB, ensure that agencies address emerging cybersecurity threats in their FISMA−required information security program and coordinate with DHS and the Department

of Justice to establish guidance for agencies on how to appropriately address and report incidents of emerging threats. OMB representatives generally agreed with GAO findings and conclusions and indicated their plans to address the recommendations.
Highlights: http://www.gao.gov/highlights/d05231high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−05−231

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT has received reports indicating an increase in the scanning for and exploitation of systems affected by one or more vulnerabilities in the Microsoft ASN.1 Library (MSASN1.DLL). These vulnerabilities are caused by the way that certain ASN.1 length values and bit strings are decoded. By sending specially crafted ASN.1 data, an attacker may be able to execute arbitrary code with SYSTEM privileges and gain complete control of a vulnerable system. **MS04−007** explains how an attacker could exploit these vulnerabilities. "Because ASN.1 is a standard for many applications and devices, there are many potential attack vectors. To successfully exploit this vulnerability, an attacker must force a computer to decode malformed ASN.1 data. For example, when using authentication protocols based on ASN.1 it could be possible to construct a malformed authentication request that could expose this vulnerability." It is possible that these attacks target Secure Sockets Layer (SSL) or other cryptographic authentication capabilities in Microsoft Internet Information Server (IIS). In addition, a number of exploit tools now include functionality to take advantage of these vulnerabilities. Microsoft has released a patch to address these vulnerabilities in Microsoft Security Bulletin MS04−007

Current Port Attacks

Top 10 Target Ports	445 (microsoft−ds), 27015 (halflife), 135 (epmap), 1026 (−−−), 53 (domain), 6881 (bittorrent), 4672 (eMule), 139 (netbios−ssn), 80 (www), 1025 (−−−) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

Nothing to report.

[Return to top]

DHS/IAIP Products & Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures:

DHS/IAIP Daily Open Source Infrastructure Reports − The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS/IAIP Daily Open Source Infrastructure Report is available on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

Homeland Security Advisories and Information Bulletins − DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact. Homeland Security Advisories and Information Bulletins are available on the Department of Homeland Security Website: http://www.dhs.gov/dhspublic/display?theme=70

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is a non−commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.